CLAIMS

1. In a network of connected devices, a communications security method comprising:

encrypting documents with a public key;

transmitting the encrypted documents to a network-connected printer;

at the printer, accepting a private key corresponding to the public key used to encrypt the documents;

decrypting the documents with the private key; and,

printing the decrypted documents.

2. The method of claim 1 wherein encrypting the documents with a public key includes encrypting the documents at a network-connected computer having a public key encryption application; and,

wherein transmitting the encrypted documents to a network-connected printer includes transmitting the encrypted documents from the computer, to the printer, through a network.

3. The method of claim 2 wherein decrypting the documents with the private key includes operating the printer in response to the printer driver encryption software; and

the method further comprising:

supplying the printer driver encryption software to the computer.

4. The method of claim 3 wherein supplying the printer driver encryption software to the computer includes:

supplying an application to optionally encrypt documents;

in response to the application, creating a graphical user interface (GUI) dialog box to invoke the document encryption option; and,

in response to invoking the document encryption option, creating a graphical user interface (GUI) dialog box to request and accept public key information.

5. The method of claim 2 further comprising:

generating a plurality of public keys with corresponding private keys;

distributing the public keys universally to network-connected computers; and,

selectively distributing the private keys.

6. The method of claim 5 in which the printer has a card reader to read code from SMART cards;

wherein selectively distributing the private keys includes distributing the private keys as SMART cards; and,

wherein accepting a private key includes using the code read by the printer card reader.

7. The method of claim 5 in which the printer has a keyboard interface to accept an alpha-numeric code, and the method further comprising:

storing the private keys in the printer;

wherein selectively distributing the private keys includes:

selectively distributing alpha-numeric codes;

creating a table in the printer to cross-reference private keys with alpha-numeric codes; and,

wherein accepting the private keys includes using the private key referenced by the entered alpha-numeric code.

8. The method of claim 2 further comprising:

spooling the encrypted documents in printer memory; and,

wherein decrypting the documents with the private key includes retrieving the encrypted documents from printer memory.

9. The method of claim 2 further comprising:

spooling the encrypted documents to a network-connected file server;

notifying the printer of encrypted documents spooled on the network file server; and,

wherein decrypting the documents with the private key includes the printer retrieving the encrypted documents from the file server.

10. The method of claim 2 further comprising:

in response to accepting the private key, generating a list of documents encrypted with the corresponding public key;

creating a graphical user interface (GUI) dialog box to invoke the selection of an encrypted document; and,

wherein printing the documents includes printing the documents in response to selecting a document.

11. The method of claim 1 wherein transmitting the encrypted documents to a network-connected printer includes transmitting a facsimile (FAX) transmission; and,

wherein decrypting the documents with the private key includes decrypting the encrypted FAX transmission.

12. A method for secure communications to a network-connected printer, the method comprising:

receiving documents encrypted with a public key;

accepting a private key corresponding to the public key used to encrypt the documents;

decrypting the documents with the private key; and,

printing the decrypted documents.

13. The method of claim 12 wherein decrypting the documents with the private key includes operating the printer in response to publicly distributed printer driver encryption software.

14. The method of claim 12 in which the printer has a card reader to read code from SMART cards; and,

wherein accepting a private key includes using the code read by the printer card reader as the private key.

15. The method of claim 12 in which the printer has a keyboard interface to accept an alpha-numeric code, and the method further comprising:

storing the private keys in the printer;

creating a table in the printer to cross-reference private keys with alpha-numeric codes; and,

wherein accepting the private keys includes using the private key referenced by the entered alpha-numeric code as the private key.

16. The method of claim 12 further comprising:

spooling the encrypted documents into a printer memory; and,

wherein decrypting the documents with the private key includes retrieving the encrypted documents from printer memory.

17. The method of claim 12 further comprising:

in response to accepting the private key, generating a list of documents encrypted with a corresponding public key;

creating a graphical user interface (GUI) dialog box to invoke the selection of an encrypted document; and,

wherein printing the documents includes printing the documents in response to selecting a document.

18. The method of claim 12 wherein receiving documents encrypted with a public key includes receiving encrypted documents transmitted as a facsimile (FAX) transmission; and,

wherein decrypting the documents with the private key includes decrypting the encrypted FAX transmission.

19. A communications security system in a network of connected devices, the system comprising:

a computer having a network connection, an input to accept a public key, and an encryption application to supply encrypted documents to the network connection in response to accepting a public key;

a network connected to the computer to receive and transmit encrypted documents; and,

a printer having an input connected to the network to accept encrypted documents, the printer having an input to accept a private key corresponding to the public key used to encrypt the documents at the computer, the printer having a decryption application to decrypt the documents with the private key, and the printer having an output to supply a printout of the decrypted documents.

20. The system of claim 19 wherein the computer includes printer driver encryption software to generate the encryption application; and

wherein the printer is operated in response to the printer driver encryptions software loaded in the computer.

21. The system of claim 20 wherein the computer has a display with an input connected to the application, wherein encryption application creates a graphical user interface (GUI) dialog box on the display to optionally invoke the encryption of documents, and in response to invoking the document encryption option, creates a GUI dialog box to request and accept public key information.

22. The system of claim 19 further comprising:

a system administrator to generate a plurality of public keys with corresponding private keys, the system administrator distributing the public keys universally to network-connected computers, and selectively distributing the private keys.

23. The system of claim 22 further comprising:

private keys configured code in SMART cards; and,

wherein the printer private key input is a card reader to read SMART cards, the printer using the code read by the card reader as the private key.

24. The system of claim 22 wherein the system administrator generates a table cross-referencing the private keys to alpha-numeric codes, and selectively distributes the alpha-numeric codes; and,

wherein the printer private key input is a keyboard interface to accept private keys referenced by the alpha-numeric code entered on the keyboard, and the printer further comprising a memory to store the private keys, and a table to cross-reference private keys to alpha-numeric codes.

25. The system of claim 19 wherein the printer includes a memory to spool the encrypted documents, the printer decrypting the documents with the private key by retrieving the encrypted documents from printer memory.

26. The system of claim 19 further comprising:

a file server connected to the network to receive encrypted documents from the computer and to transmit encrypted documents to the printer; and,

wherein the printer decrypts documents with the private key after retrieving the encrypted documents from the file server.

27. The system of claim 19 wherein the printer has display connected to the decryption application to depict a list of documents encrypted with a corresponding public key, in response to accepting the private key;

wherein the printer decryption application creates a GUI dialog box on the display to invoke the selection of encrypted documents, the printer printing the documents in response to selecting a document from the GUI dialog box.

28. The system of claim 19 wherein the computer transmits the encrypted documents as a facsimile (FAX) transmission;

wherein the network is a telephone system; and,

wherein the printer decrypts the encrypted FAX transmission.

29. A secure communications network-connected printer, the printer comprising:

a network connection to receive documents encrypted with a public key;

an input to accept a private key corresponding to the public key used to encrypt the documents;

an decryption application to decrypt the documents with the private key; and,

an output to supply a printout of the decrypted documents.

30. The printer of claim 29 wherein the decryption application is responsive to publicly distributed printer driver encryption software.

31. The printer of claim 29 wherein the private key input is a card reader to read code from SMART cards.

32. The printer of claim 29 wherein the private key input is a keyboard interface to accept an alpha-numeric code; and,

the printer further comprising:

a memory to store the private keys;

a memory to store a table cross-referencing private keys with alpha-numeric codes; and,

wherein private key input uses the private key referenced by the alpha-numeric code entered at the printer keyboard.

33. The printer of claim 29 further comprising:

a memory to spool the encrypted documents; and,

wherein decryption application retrieves the encrypted documents from printer memory for decryption.

34. The printer of claim 29 further comprising:

a display having an input;

wherein the decryption application creates a graphical user interface (GUI) dialog box application on the display to invoke the selection of an encrypted document, the GUI generating a list of documents encrypted with a corresponding public key, in response to accepting the private key; and,

wherein the documents are decrypted and printed in response to the documents being selected from the GUI.

35. The system of claim 29 wherein the network connection is a telephone connection and the encrypted documents are facsimile (FAX) transmissions; and,

wherein the printer decrypts the encrypted FAX transmission.